Robust Grey-Scale Image Watermarking Using Two Dimensional Walsh Coding

Kamal A. Ahmed*[1], Hussain Al-Ahmad[2], Patrick Gaydecki[3]

[1]School of Electrical and Electronic Engineering, University of Manchester, UK, [2]Department of Electronic Engineering, Khalifa University of Science, Technology and Research, Sharjah, UAE, [3]School of Electrical and Electronic Engineering, University of Manchester, UK

*[1]kamal.ahmed@postgrad.manchester.ac.uk; [2]alahmad@kustar.ac.ae; [3]patrick.gaydecki@manchester.ac.uk

Abstract

1-D Walsh coding was presented to improve the robustness of digital image watermarking. In this paper, an efficient, new two dimensional Walsh code approach to copyright protection is proposed. The proposed technique inserts the Walsh coded binary bits of handwritten signatures in the DCT blocks of the 512×512 grey scale colour images. The embedding procedure is realized by transforming the host image into DCT domain. The low frequency coefficients of the DCT blocks undergo modification by inserting the Walsh coded watermark. The algorithm is blind and does not require the original image in the extracting process. The distortion caused by the watermarking algorithms is invisible and it has been assessed by using the PSNR and SSIM. The empirical results show the effectiveness of the proposed scheme to accomplish high imperceptible quality watermarked image and smooth watermark detection. The robustness of the algorithm has been verified using Stir Mark benchmark and other conventional attacks. The watermark recovery is achieved 100% even by using significant JPEG compression and some common signal processing attacks.

Keywords

WaterMarking; DCT; Walsh Coding; Grey Scale Image; Zena Image

Introduction

The availability of personal computers and the internet has caused an increase in media piracy along with the prevailing of copying and modifying files and documents. The illegal copying of some types of media has been a subject of concern for many years. As a result, an urgent solution to copyright protection and authentication is needed. Digital watermarking is an effective solution to protect intellectual properties and copyrights by hiding information such as logos, signatures or text into multimedia data such as images, videos, or audio files.

Watermarked images must not be visibly degraded by the presence of the watermark information. The degradation can be assessed subjectively by inspecting the watermarked images. The objective assessment can be done by using the peak signal to noise ratio (PSNR) and the structured similarity index measure (SSIM) (Wang Hou, 2004). As well the watermarking algorithm must be robust in order to protect the embedded information inside the host images. Thus, the watermark must be resistant to unauthorized detection and decoding. In addition, the watermark must be tolerant to image processing techniques such as compression as well as to intentional attempts to destroy or remove the watermark such as filtering operations.

Digital watermarking can be classified according to the insertion domainwhich is either the spatial domain or the transformed domain. In the spatial domain, the watermark can be embedded by using the least significant bits (LSB) technique. The transformed domain algorithms are more robust compared to the spatial domain ones. Examples of transform domains are the discrete Fourier transform (DFT), discrete cosine transform (DCT), and discrete wavelet transform (DWT) (Barni M., 1998, Katzenbeisser S., 2000, Lin P-L., 2000). The DCT domain is the most popular one for image watermarking because of the wide use of the JPEG compression algorithm. Watermarks may also be classified as robust and fragile. Robust watermarks are those which are difficult to remove from the object into which they are embedded, despite various attacks they might be subjected to. Fragile watermarks are those that are easily destroyed by any attempt to tamper with them. Fragile watermarking is used to check the authenticity of the image. Another classification is based on the availability of the original image during the extraction process. The algorithm is called blind if the original

image is not required to recover the watermark, otherwise, non-blind.

One dimensional Walsh coding was used to improve the robustness of the digital watermarking algorithms working in the DCT domain (Ahmed K., 2009, Ahmed K., 2011). 2D Walsh coding was also used for the same purpose (Bin Sewaif A., 2004). However, the 2D algorithm was non-blind. In this paper a new blind technique using 2D Walsh coding will be presented. The new algorithm will use handwritten signatures as the watermarking information. The paper consists of five sections. Section 2 introduces Walsh coding functions and also the DCT watermarking technique using the low frequency coefficients. In section 3, experimental results are discussed. in section 4, conclusions are drawn. Finally a comparison is carried out between the proposed algorithm and existing methods in section 5.

The New 2D Algorithm

Walsh Coding

Walsh functions that are orthogonal sequences and contain different length elements, consist of square pulses with two states either +1 or –1. Walsh sequences with length k, where $k=2^n$, enable k orthogonal codes to be obtained. There are several ways to produce Walsh sequences, of which the easiest involves manipulations with Hadamard matrices. Walsh functions with length k= 4 as shown below are used in this paper (Ahmed K., 2012).

$$\begin{aligned} \mathbf{w}_1 &= [+1 \quad +1 \quad +1 \quad +1] \\ \mathbf{w}_2 &= [+1 \quad +1 \quad -1 \quad -1] \\ \mathbf{w}_3 &= [+1 \quad -1 \quad -1 \quad +1] \\ \mathbf{w}_4 &= [+1 \quad -1 \quad +1 \quad -1] \end{aligned} \qquad (1)$$

Binary signatures are used as the watermarking information. The signature can be divided into 4x4 blocks. In the first stage, 1D Walsh coding is multiplied with the elements of each row of the block. The resultant codes are multiplexed to generate a 4x4 block. The element of this block will be decimal numbers in the range of 2 to 4. The resulting 1D coded block is taken as an input to the second stage. In the second stage, 1D Walsh coding is multiplied with the elements of each column of the input 1D coded block and then multiplexed to generate the 2D Walsh coded block. Each element of the 2D Walsh coded block is a decimal number in the range of 8 to 16. These decimal numbers are converted into binary numbers using 5 bits as shown in Figure 1.

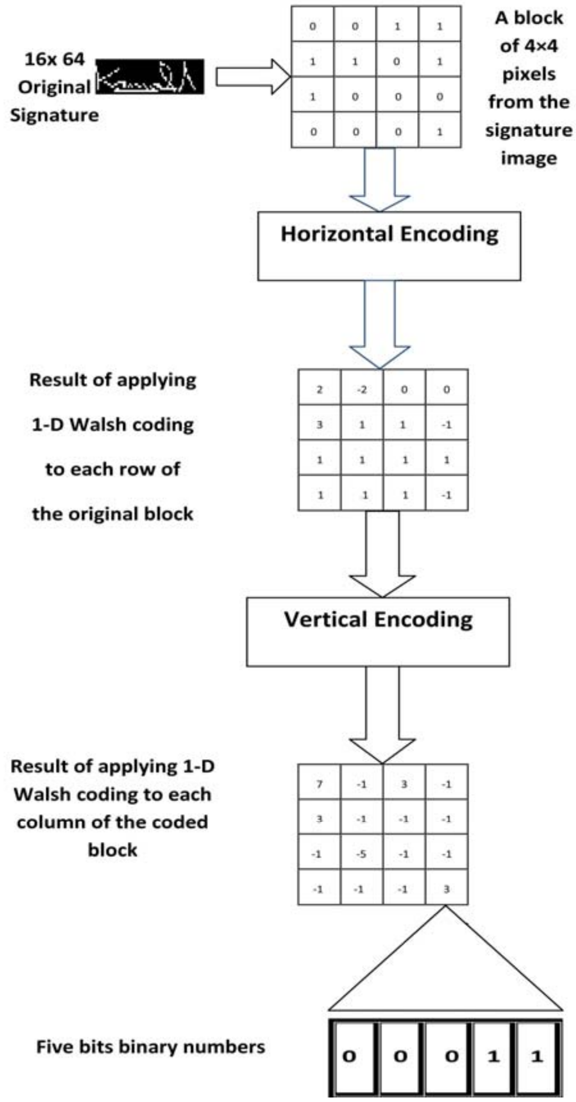


FIG. 1 WALSH CODING OF HANDWRITTEN SIGNATURE

DCT Embedding

The cover image is divided into 8×8 DCT blocks. The low frequencies are screened to find the coefficients with the highest values and their locations are defined. The locations will vary from one image to another according to the spatial frequency contents of the image. Five low-frequency coefficients excluding the dc component of the 8×8 DCT blocks will be used to hide the watermark bits. The coefficients are divided by a scaling factor and the embedding process is achieved by changing the value of the coefficient into odd or even numbers. The same procedure is repeated for the other DCT blocks. Then the inverse DCT is used to construct the watermarked image (Al-Gindy A , 2009, Al-Gindy A , 2009, Barni M., 1998) as shown in Figure 2.

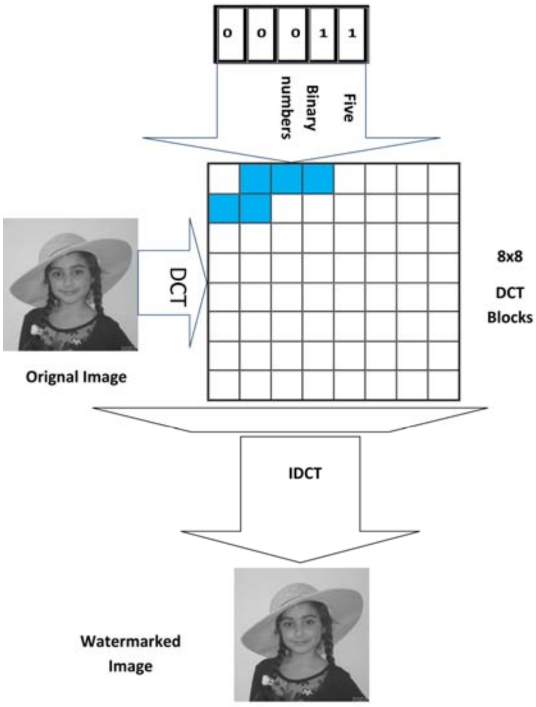


FIG. 2 DCT BLOCK ENCODER in THE FREQUENCY DOMAIN

Watermark Detection

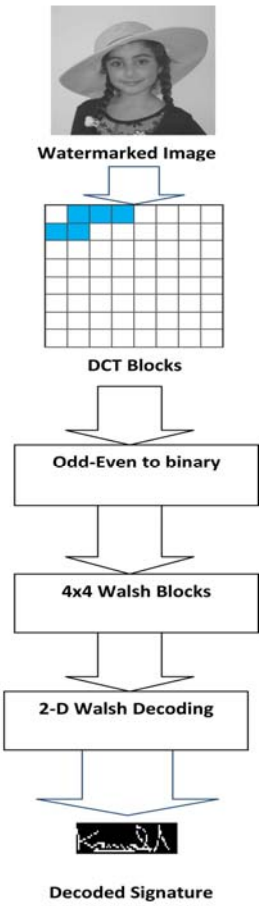


FIG. 3 The EXTRACTION PROCESS

The decoding process works as follows: first is to convert the watermarked image into 8×8 blocks and apply the DCT to each block. Then the watermarked coefficients are located and checked to see whether they are even or odd. The five binary bits are extracted and used to construct the (4×4) 2D Walsh block with decimal numbers. The (4×4) 2D Walsh block is decoded to construct the binary signature as shown in Figure 3.

Results and Discussion

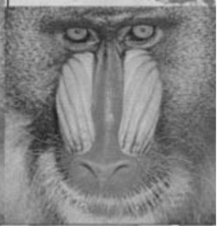
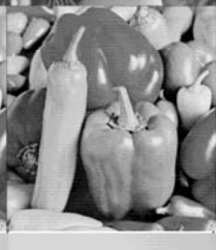
Image Scale= 20	Original Standard Image	Watermarked Image
Airplane PSNR=35.8034 SSIM=0.9058		
Baboon PSNR=35.5330 SSIM=0.9548		
Lena PSNR=35.5938 SSIM=0.9127		
Peppers PSNR=35.6095 SSIM=0.9133		
Zena PSNR=36.2283 SSIM=0.8873		

Fig. 4. TEST IMAGES AND THEIR WATERMARKED VERSION

This algorithm has been examined using different 8 bits gray level images of size 512×512 pixels and different handwritten signatures of size 16x64. Figure 4 shows the original and the watermarked images. Investigation is carried out to assess the fidelity of the images by using the PSNR and SSIM. Table 1 shows

the PSNR and SSIM values of different images using the new algorithm with different strengths. Table 2 shows the lowest JPEG quality below which the handwritten signature is not recognisable as function of the watermark strength. The effect of the scaling factors on the perceptual invisibility is studied by using the PSNR and SSIM. Table 1 also demonstrates the effect of the scaling factors from 4 to 20 on the perceptual invisibility of the watermarked images with Walsh length of 4. The PSNR values are in between 35.53 dB and 49.63 dB. The results show that increasing the value of scaling factor will affect the quality of the watermarked image. Similarly from Table 1 the values of the SSIM are in the range from 0.8873 to 0.9980. It is clear that the distortion caused by the new watermarking scheme is invisible in all tested images.

TABLE 1 PSNR AND SSIM WITH WALSH 4

Scaling factor	SSIM	PSNR
Aeroplane Image		
4	0.9950	49.5484
8	0.9811	43.5965
12	0.9601	40.0597
16	0.9340	37.6211
20	0.9058	35.8034
Baboon Image		
4	0.9980	49.4960
8	0.9922	43.4965
12	0.9827	39.9750
16	0.9699	37.4004
20	0.9548	35.5330
Lena Image		
4	0.9956	49.4926
8	0.9829	43.3921
12	0.9634	39.8894
16	0.9399	37.4608
20	0.9127	35.5938
Peppers Image		
4	0.9957	49.4749
8	0.9839	43.5747
12	0.9646	39.9857
16	0.9406	37.4653
20	0.9133	35.6095
Zena Image		
4	0.9935	49.6396
8	0.9778	43.9722
12	0.9539	40.5609
16	0.9232	38.1457
20	0.8873	36.2283

From Table 2, it is also shown that the signature can be recovered with a scaling factor of 4 with JPEG quality > 90. As the scaling factor is increased then the robustness is improved and at scaling factor of 20 the signature can be recovered with JPEG quality > 27. The results show that the proposed algorithm is robust against the JPEG attack. It should be noted that there should be a compromise between the robustness and the distortion caused to the watermarked images. The algorithm is tested using the Stir mark software to assess the robustness against other attacks. The testing is done on the standard image of Lena with scaling factor 20. Table 3 shows the Stir mark attacks and their normalised correlation (NC) values.

The execution time of the algorithm using MATLAB, an Intel CPU@ 2.2Ghz Centrino processor and 4 Gb memory is approximately 4.3 seconds.

TABLE 2 THE LOWEST JPEG FACTORS WITH WALSH 4

Scaling factor	JPEG factor(Q)	Recovered signature at Scale =20
Aeroplane Image		
4	84	
8	66	
12	49	
16	38	
20	29	
Baboon Image		
4	84	
8	70	
12	52	
16	38	
20	29	
Lena Image		
4	83	
8	70	
12	50	
16	36	
20	27	
Peppers Image		
4	89	
8	67	
12	48	
16	37	
20	27	
Zena Image		
4	90	
8	67	
12	48	
16	36	
20	27	

TABLE 3 STIR MARK ATTACKS AND THEIR NORMALISED CORRELATION (NC) VALUES WITH WALSH 4

Attack	NC
Additive noise 0.1	0.9875
Additive noise 0.3	0.9875
Additive noise 0.5	0.9875
Additive noise 0.7	0.9875
Additive noise 0.9	0.9875
JPEG 20	0.9659
JPEG 25	0.5289
JPEG 30	0.9852
JPEG 75	0.9875
Median 3x3	0.8876
Median 5x5	0.9921
PSNR 30	0.9875
PSNR 50	0.9875
PSNR 70	0.9875
PSNR 90	0.9875
Rotation 0.25	0.9973
Rotation 0.5	0.9909

Comparison

In previous section, the performances of the proposed scheme was assessed in terms of robustness and watermarked image fidelity. This was done using a range of simulation tests which have shown that the proposed scheme is robust and secure against JPEG compression and a wide range of image processing operations. To validate the above scheme, comparison will be run between the proposed scheme and some methods in the literature. The peak signal to noise ratio (PSNR) was adopted to quantify the similarity between the original grey image and the watermarked image. The normalised correlation (NC) was also employed to measure the similarity between the original watermark and the corrupted watermark. To carry out this assessment, two comparisons were made between the proposed scheme and existing methods (Xiaochuan Gao, 2006, Gaorong Zeng, 2008). In this evaluation, a standard 512×512 colour Lena image was used in conjunction with watermarks of dimensions 32×32 and 64×64 pixels.

The first comparison was carried out between the proposed algorithm and method in (Xiaochuan Gao, 2006) to validate the scheme. Robustness and watermarked image fidelity were also assessed using the proposed algorithm against the method described in (Xiaochuan Gao, 2006) to confirm validity. 512×512 grey scale image and a 32×32 watermark were used. From table 4, the value of PSNR and NC of the watermarked image in method in (Xiaochuan Gao, 2006) before attack are 35.7, 1 respectively, while the value of PSNR and NC in the proposed algorithm is: 52.96, 1 respectively, which is higher. Table 4 shows also a comparison of robustness to JPEG compression between the two methods. When the JPEG attack of quality factor of 50, the PSNR and NC in method in (Xiaochuan Gao, 2006) are 35.34, 0.99 respectively, while the value of PSNR and NC in the proposed algorithm is 41.55, 1 respectively, which is also higher.

Similarly, the JPEG quality factors of 30 down to 20; in the case of the algorithm in (Xiaochuan Gao, 2006), a considerable fall in the value of NC takes place. While with the proposed algorithm, under all these JPEG values of attacks, 100% watermark detection is guaranteed whilst maintaining a high quality of PSNR. Table 4 shows the perfect detection of the watermark image in almost all attacks including Gaussian noise and cropping, providing the highest value of NC. Apart from the median filter attack, the PSNR values of the watermarked Lena image are all higher than the values in the reference method. However, the proposed algorithm offers maximum trade off between the perceptual distortion caused by embedding and tolerance against certain attacks.

Another comparison was carried out between the proposed algorithm and the method described in ((Gaorong Zeng, 2008) to confirm validity in term of robustness and watermarked image quality. 512×512 grey scale Lena image and a 64×64 watermark were adopted. In table 5, the value of PSNR and NC of method in (Gaorong Zeng, 2008) before attack are 44.26, 1 respectively, while the value of PSNR and NC in the proposed algorithm is 50.51, 1 respectively, which is higher. Table 5 shows also a comparison of robustness to JPEG compression between the two methods. When the JPEG attack of quality factor of 65 and 50, the PSNR and NC in method in (Gaorong Zeng, 2008) are 39.03, 1, and 38.29, 0.9569 respectively, while the value of PSNR and NC in the proposed algorithm is 43.05, 1 and 40.46, 1 respectively, which is also higher. Table 5 demonstrates as well the values of PSNR and NC of the proposed algorithm and method in (Gaorong Zeng, 2008) in case of median filter and the Salt and Pepper, at which the method in (Gaorong Zeng, 2008) acquired higher values. In case of the Gaussian attack both method have the same values of PSNR and NC, while higher values of PSNR and NC are achieved by the proposed algorithm when cropping attack is applied.

The above analysis illustrates that the proposed algorithm outperforms other watermarking methods for tests involving JPEG compression. Furthermore the

PSNR rate of watermarked images without attack is always superior. In summary, use of the Walsh code prior to embedding ensures that the algorithm performs better than those that do not employ such an encoding scheme.

TABLE 4 COMPARISON BETWEEN THE PROPOSED ALGORITHM AND METHOD IN [13]

Attack	Method in [13]		proposed scheme	
	PSNR	NC	PSNR	NC
No attack	35.7	1	52.96	1
JPEG 50	35.34	0.99	41.55	1
JPEG30	33	0.98	37.31	1
JPEG25	23.57	0.70	35.60	1
JPEG20	14.6	0.40	34.15	1
Median filter 3×3	35.00	0.9600	27.09	1
Gaussian noise 0.001	22.80	0.92	28.80	1
Gaussian noise 0.002	21.31	0.86	26.83	1
Cropping 25%	12.40	0.74	50.43	0.9671

TABLE 5 COMPARISON BETWEEN THE PROPOSED ALGORITHM AND METHOD IN [9]

Attack	Method in [9]		proposed scheme	
	PSNR	NC	PSNR	NC
No attack	44.26	1	50.51	1
JPEG 65	39.03	1	43.05	1
JPEG 50	38.29	0.9569	40.46	1
Median filter 3×3	38.60	0.8913	32.94	0.7703
S & P 0.001	44.04	0.8869	38.51	0.8468
Gaussian noise 0.0005	35.20	0.8014	35.00	0.8153
Cropping attack	32.08	0.6267	43.39	0.9546

Conclusions

A blind watermarking algorithm for gray level still images using 2D Walsh coding has been proposed. The algorithm embeds the watermark in five low frequency DCT coefficients. It was found that the use of the 2D Walsh code improved the robustness against JPEG compression and some other attacks such as additive noise, cropping and filtering. Comparison has been made between the proposed algorithm and other methods in the literature to examine the image fidelity and evaluate robustness. The results show that the Walsh 2D can reach higher values of PSNR and NC respectively, meaning that the perceptual quality of images using the 2D is better than the schemes without Walsh codes. In case of robustness, the results show that the Walsh 2D can survive with lower values of quality factor.

Although the scheme presented is quite transparent and robust against many image processing attacks, it is vulnerable to geometric attack such as rotationdue to the fact that the DCT is very sensitive to rotation (since it generates both horizontal and vertical components). Further development in this direction is required. One possibility is by means of exploition of the polar representation of a transform, in which only magnitudes would become significant. The algorithm was examined using standard grey scale images comprising 256×256 and 512×512 pixels, in conjunction with watermarks with dimensions of 16×64, 32×32 and 64×64 pixels. Further work will concentrate on the use of higher resolution images such as 1024×1024 and 2048×2048 pixels to assess its performance.

REFERENCES

Ahmed. K. A., H. Al Ahmad, and P. Gaydecki, ROBUST IMAGE WATERMARKING USING TWO DIMENSIONAL WALSH CODING, The IET Image Processing Conference 2012, London, 2012, pp. 1 - 5

Ahmed K., A. Ahmed H. Al Ahmad, P. Gaydecki, “A Blind Block Based DCT Watermarking Technique for Gray Level Images Using One Dimensional Walsh Coding”, International Conference on Current Trends in Information Technology (CTIT), December 2009, pp.79-84

Ahmed. K. A., H. Al Ahmad, and P. Gaydecki, “1-D Walsh Coded Watermarking Technique for Colour Images Using the Y Chanel”, 2011 IEEE GCC Conference and Exhibition, Dubai, UAE, February 2011, pp.299-302

Al-Gindy A., A. Tawfik H. Al- Ahmad and R. Qahwaji, ”Enhanced DCT Based Technique with Shuffle Scheme For Robust Image Watermarking of Handwritten Signatures”, Inter-national Conference for Communication, Computer and Power (ICCCP), Oman, February 2007, pp.450-455

Al-Gindy A., A. Tawfik H. Al- Ahmad , R. Qahwaji and A. Tawfik, “A New Watermarking Scheme For Color Images Captured By Mobile Phone Camera”, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.7, pp2480254, July 2009

Al-Gindy A., H. Al-Ahmad, R. Qahwaji and A. Tawfik, “Watermarking of Color Images in the DCT Domain Using Y Channel”, IEEE/ACS International Conference on Computer Systems and Applications, pp.1025-1028, May 2009

Barni M., F. Bartolini, V. Cappellini, and A. Piva, “A DCT-Domain System for Robust Image Watermarking,” Signal Processing, vol. 66, 1998, pp. 357–372

Bin Sewaif A., H. Al-Ahmad, and M. E. Al-Mualla, "2-D Walsh Coding for Robust Digital Image Watermarking," Siignal Processing and Information Technology(ISSPIT), December 2004

Gaorong Zeng, Zhengding Qiu,"Image Watermarking Based on DC Component in DCT", International Symposium on Intelligent Information Technology Application Workshops, IEEE, 2008, pp 573-576

Katzenbeisser S., and F. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, London, 2000

Lin P-L., "Robust Transparent Image Watermarking System with Spatial Mechanisms", The Journal of Systems and Software, vol. 50, 2000, pp. 107–116

Wang Hou, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli "Image Quality Assessment: From Error Visibility to Structural Similarity", IEEE Transaction on Image Processing, Vol.13, No.4, April 2004, pp.600-612

Xiaochuan Gao, Chun Qi, Haitao Zhou,"An Adaptive Compressed-DCT-Domain Watermarking", ICSP2006 Proceedings, IEEE, 2006, Vol.4